Kryptographie

Rosa Freund <rosa@pool.math.tu-berlin.de>

D466 2926 104B 820E DD7F 6956 5E63 529D E219 AC59

30. September 2006

Zeitplan

- Einführung, Geschichte, Grundlagen der Kryptographie.
- Web of Trust, PKIs, PGP, SSL.
- Praxis! Erstellen von PGP-Schlüsseln, Schlüsselaustausch, Verschlüsseln, Entschlüsseln, Signieren.

Fragen

- Kurze Vorstellungsrunde:
- Wofür nutzt Ihr bisher Verschlüsselung? Warum? Warum nicht?
- Was erhofft Ihr Euch vom Kurs? Was interessiert Euch besonders?

Ziele kryptographischer Verfahren

- **Datenschutz**: Ich möchte, dass eine Nachricht nur vom vorgesehenen Empfänger gelesen werden kann.
- **Authentizität**: Ich möchte feststellen können, ob eine Nachricht tatsächlich von einem bestimmten Absender stammt.
- **Integrität**: Ich möchte feststellen können, dass eine Nachricht auf ihrem Weg zu mir nicht verändert wurde.
- **Lösung**: Verschlüsseln und Signieren.

Allgemeines

Zum verschlüsselten Kommunizieren benötigen die Parteien

- Ein Verschlüsselungsverfahren, mit dem ver- und entschlüsselt wird (z.B. PGP, SSL)
- Einen oder mehrere Schlüssel, d.h. den Variablen, die das Verfahren benötigt, müssen Werte zugeordnet werden
- Z.B. Verschlüsselungsverfahren Cäsarchiffre, Schlüssel ist die Zahl, um die das Alphabet verschoben wird

Geheime Botschaften

- Kryptographie

  vs.

- Steganographie

Kerckhoff-Prinzip

- Auguste Kerckhoff, 1883: *La Cryptographie militaire*
- Sicherheit eines kryptographischen Systems sollte nur auf der Geheimhaltung des Schlüssels beruhen, nicht jedoch auf Geheimhaltung des Verfahrens selbst
- Vorteile: die Qualität des Verfahrens kann intensiver untersucht werden

Kryptographie in der Geschichte (in Auszügen)

- 52 v.Chr.: Cäsarchiffre (monoalphabetisch)
- 16. Jhdt.: Vigenèrechiffre (polyalphabetisch)
- 2. Weltkrieg: Enigma (Walzensystem, polyalphabetisch)
- seit 1976: Public-Key-Kryptographie

Vigenèrechiffre

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Quelle: Wikimedia Commons

Warum verschlüsseln?

- „Ich habe doch nichts zu verbergen?“
- „Nothing to hide, but something to protect!“

Gesetzgebung

- z.B. USA: Verbot des Exportes kryptographischer Verfahren.
- z.B. Russland, China: Benutzung „starker Kryptographie“nur mit staatlicher Lizenz legal, verboten für Privatanwenderinnen.
- z.B. UK: Rechtliche Möglichkeit, die Herausgabe von privaten Schlüsseln durchzusetzen.

Symmetrische Verfahren

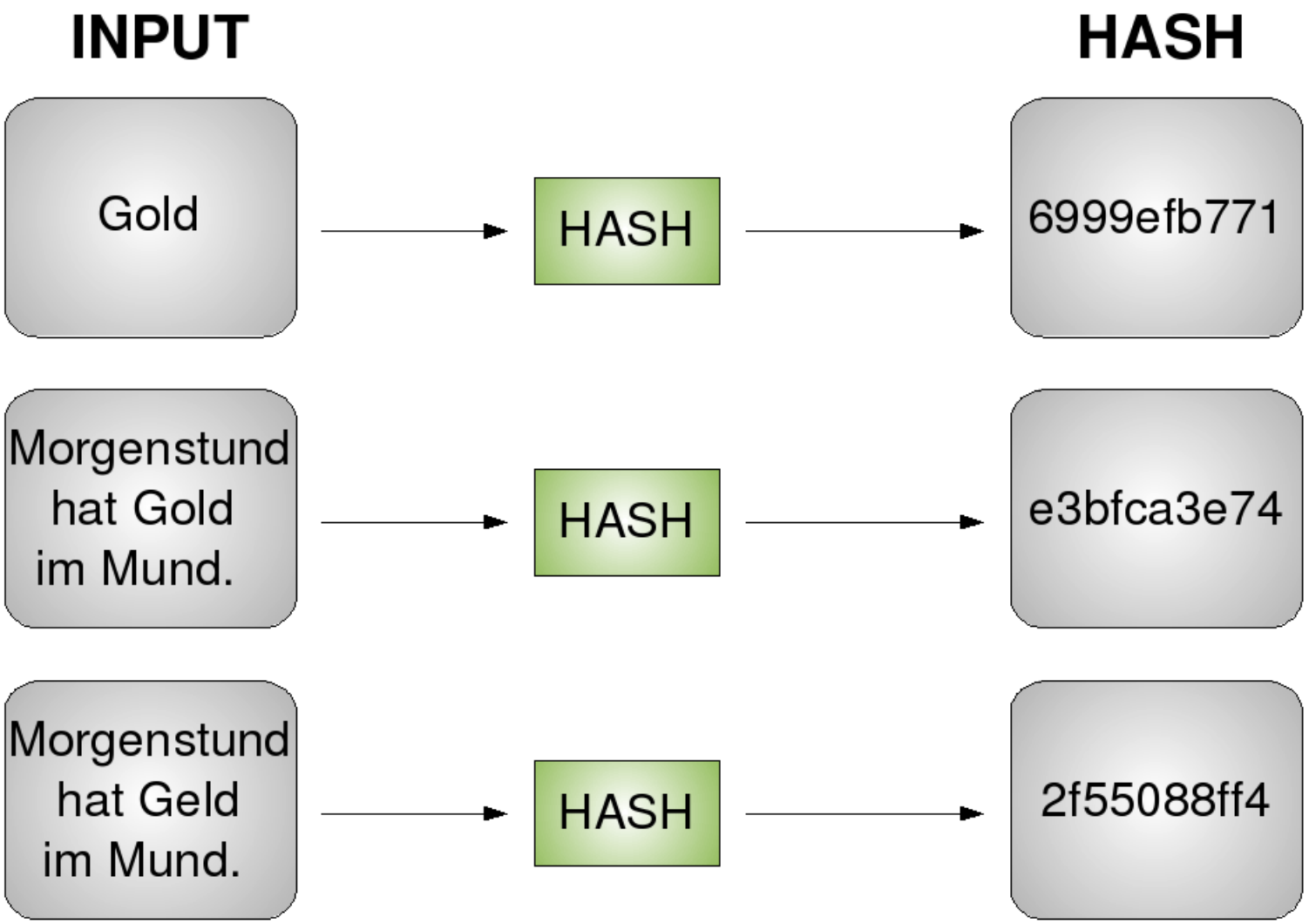
- Die kommunizierenden Parteien teilen sich einen geheimen Schlüssel (secret key)
- Z.B. One-Time-Pad, Blockchiffren (DES, AES), Enigma
- Problem: **Schlüsseltausch**

Blockchiffren

- symmetrisch
- Jede Nachricht wird in gleichlange Blöcke aufgeteilt, die Blöcke werden separat und unterschiedlich verschlüsselt. Der letzte Block wird ggf. mit Bits gepadded
- z.B. DES (1977), AES / Rijndael (2001)

Hashfunktionen 1

- Berechnet für Inputs beliebiger Länge Hashwerte von vorgegebener (meist kurzer) Länge
- Keine Entschlüsselung
- Geringe Änderung des Inputs führt zu stark geändertem Hashwert
- Weitere Merkmale: Kollisionsarmut, nicht umkehrbar, eindeutig


INPUT
HASH
Gold
HASH
6999efb771
Morgenstund hat Gold im Mund.
HASH
e3bfca3e74
Morgenstund hat Geld im Mund.
HASH
2f55088ff4

Hashfunktionen 2

- Beispiele: **MD5** (seit 2004 bekannt, dass Kollisionsangriffe möglich), **SHA-1** (seit Anfang 2005 bekannt, dass Kollisionsangriffe möglich, praktisch noch nicht von Bedeutung), **SHA-2** (bislang als sicher eingestuft)

- Anwendungen z.B.: Unix-Passworte (aber: Dictionary-Attacke), Prüfsummen (z.B. genutzt um bei Datei-Download Korrektheit der Datei zu überprüfen).

Asymmetrische Verfahren 1

- Diffie und Hellman, 1976: *New Directions in Cryptography*
- Alle Nutzenden besitzen einen öffentlichen sowie einen geheimen Schlüssel (**public key**, **private key**). Der Geheime ist schwer oder garnicht aus dem Öffentlichen berechenbar
- Um verschlüsselte Nachrichten erhalten bzw. Nachrichten signieren zu können, generiert Alice sich einen öffentlichen und einen geheimen Schlüssel
- Wie der Name sagt, muß Alice den geheimen Schlüssel (private key) geheimhalten, den öffentlichen (public key) jedoch veröffentlichen.

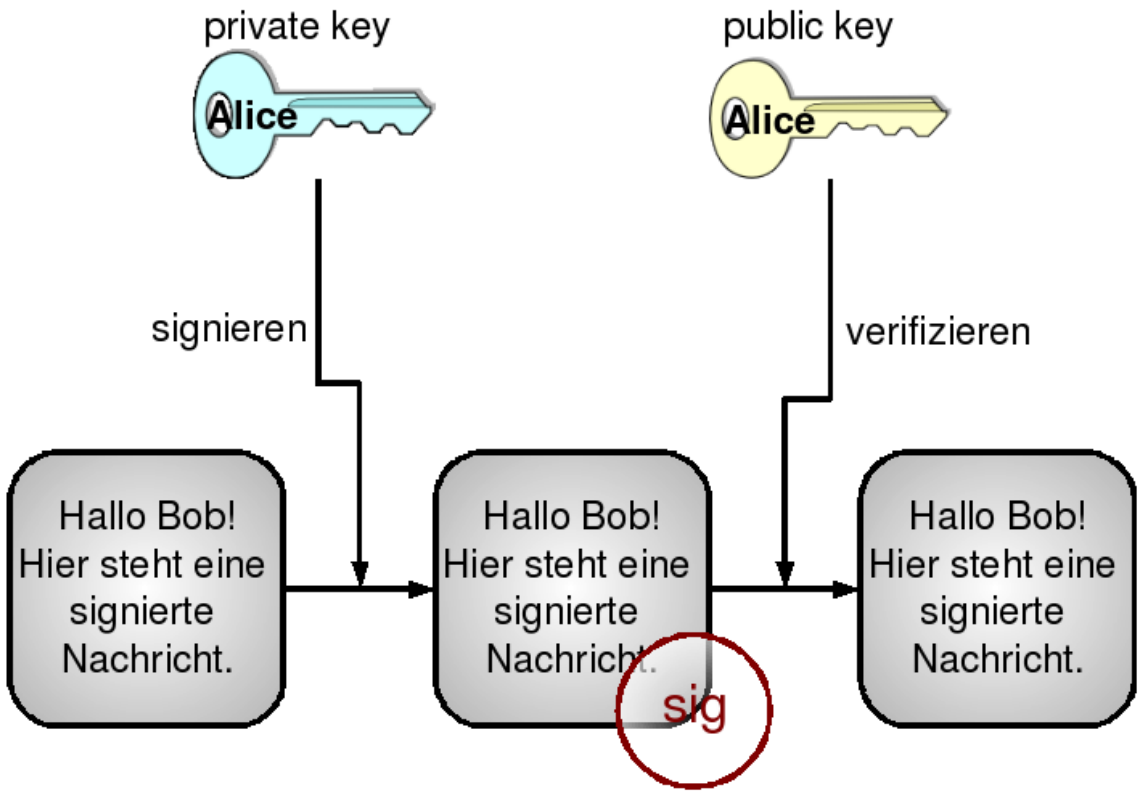
Asymmetrische Verfahren 2

- Beim **Signieren** signiert Alice die Nachricht mit ihrem geheimen Schlüssel. Bob benutzt Alices öffentlichen Schlüssel, um die Signatur zu verifizieren

- Beim **Verschlüsseln** nutzt Bob den öffentlichen Schlüssel von Alice, um eine Nachricht an Alice zu verschlüsseln. Alice entschlüsselt die Nachricht mit ihrem geheimen Schlüssel

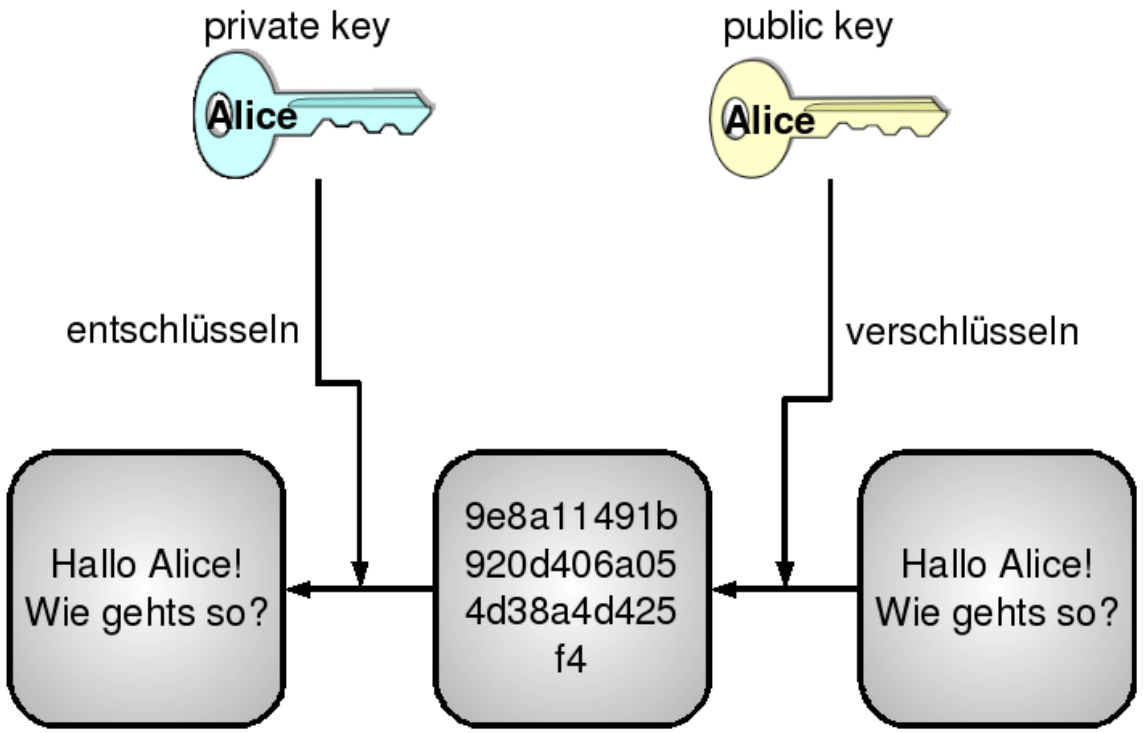
Signieren

ALICE **BOB**



Verschlüsseln

ALICE **BOB**



Asymmetrische Verfahren 3

- Sicherheit beruht meist auf algorithmischen Problemen mit hoher (bzw. ungeklärter) Komplexität
- Mathematisch geht insbesondere algebraische Zahlentheorie ein (z.B. RSA, diskretes Logarithmusproblem, elliptische Kurven)
- Häufig zum Austausch von Schlüsseln für symmetrische Verfahren genutzt (z.B. SSL), da weniger effizient als symmetrische Verfahren

Vertrauen

- Wenn ich eine Person persönlich kenne, und sie mir ihren öffentlichen Schlüssel selbst übergibt, kann ich ihr vertrauen.

- Problem: Wie kann ich öffentlichen Schlüsseln von Personen vertrauen, die mir nicht persönlich bekannt sind, oder von denen ich die öffentlichen Schlüssel per Mail oder via einem Keyserver erhalte?

- Lösung: Web of Trust und Keysigning.

Physikalische Aspekte

- **Quantenkryptographie**. Idee: Ein Nachrichtenstrom verändert sich, wenn er beobachtet wird ($\rightarrow$ Unschärferelation)

- **Quantencomputer**. Die Sicherheit der momentan gängigen Verfahren beruht auf schwierigen Algorithmen (d.h. nicht in polynomieller Laufzeit lösbar), und der Annahme $P \neq NP$. Mit Quantencomputern sind exponentielle Laufzeiten kein Problem mehr. Es wird bereits jetzt an „quantum-hard cryptography“gearbeitet.

Effizienz / Komplexität 1

- Ein Verschlüsselungsverfahren heißt effizienter als ein anderes, wenn sein Algorithmus eine niedrigere Komplexität aufweist. Es ist also in der Regel schneller berechenbar.

- Für viele Probleme ist ein Algorithmus mit **polynomieller** Laufzeit bekannt (Schreibweise z.B. $O(n^2)$). Für andere Probleme konnten lediglich Algorithmen mit **exponentieller** Laufzeit gefunden werden (z.B. $O(2^n)$). Allerdings kann bislang nicht bewiesen werden (!), dass für diese Probleme kein polynomieller Algorithmus existiert.

- Es ist also unklar, ob es wirklich zwei Klassen von Problemen gibt: polynomiell, und nicht-polynomiell lösbare.
  Andere Schreibweise: Gilt $P \neq NP$?

Effizienz / Komplexität 2

- In NP: Finde die Primfaktoren einer natürlichen Zahl, Dreifarbenproblem.
- Viele Probleme, für die kein polynomieller Algorithmus bekannt ist, sind polynomiell äquivalent. Wird für nur eins dieser Probleme ein polynomieller Algorithmus gefunden, sind die anderen Probleme auch polynomiell lösbar, und $P = NP$
- Public-Key-Verfahren beruhen meist auf Problemen aus NP. Falls also $P = NP$ gilt, wird ein Großteil der Public-Key-Kryptographie unsicher, da effizient lösbar.
- Dies ist unwahrscheinlich, aber nicht unmöglich.

Also:

- Symmetrische Verschlüsselungsverfahren sind viel effizienter (also schneller) berechenbar als asymmetrische. Problem bei symmetrischen Verfahren: Schlüsseltausch.
- Asymmetrische Verfahren beruhen darauf, dass $P = NP$ unbewiesen ist. Quantencomputer und -kryptographie sind von der Anwendung noch Jahre bzw. Jahrzehnte entfernt.
- **Jetzt**: Noch Fragen?
- **Dann**: PGP: Theorie.